Frequently Asked Questions

Complying with the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (N-CIPA)

(June 7, 2001)

The Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (N-CIPA) passed Congress in December of 2000. Both were part of a large federal appropriations measure (PL 106-554). See the "Sources" section at the end of this document for references to more information on this legislation.

This FAQ focuses specifically on issues of compliance with CIPA and N-CIPA for Year 4 of the E-rate. The questions and answers are based on discussions held among state E-Rate coordinators regarding CIPA and N-CIPA. Some of the information is also a result of conference calls between state E-rate coordinators and the FCC and SLD. The Indiana State Library has made reasonable attempts to ensure the accuracy of this information as of the date of this FAQ. However, the FCC and SLD are still working on the details of implementing CIPA and N-CIPA. Some of the information provided in this FAQ may change as the result of further clarifications made by the FCC and SLD. Only the information provided on the FCC and SLD Websites should be considered official. Readers are also encouraged to visit the ALA CIPA website, which has considerable information on this topic. These Web sites are listed at the end of this FAQ.

If, after reading this FAQ, you have any questions on the legislation, you can contact Martha Roblee, 800-451-6028 or email marthar@statelib.lib.in.us Updated versions of this FAQ will be on the State Library Website at <http://www.statelib.lib.in.us/LDO >.

CIPA and N-CIPA: There is some overlap in language between these two sections of PL 106-554. The Children's Internet Protection Act addresses the filtering requirement and the need for an Internet Safety Policy. The Neighborhood Children's Internet Protection Act focuses on what has to be included in a school or library Internet safety policy. Moreover, N-CIPA is applicable only to the E-rate program. In this FAQ the term "CIPA" is used to represent both CIPA and N-CIPA unless noted otherwise.

Federal Programs: Although CIPA compliance impacts specific use of funds from three federal programs (E-rate, ESEA Title III [TLCF], and LSTA), at this time regulations have been written only for the E-rate program. Thus, this FAQ focuses primarily on CIPA issues and compliance related to the E-rate.

Please note that this document is basically a work effort of Bob Bocher, of Wisconsin's Dept of Public Instruction, and a fellow member of the ALA E-rate Task Force. With his permission it has been edited to reflect Indiana public library needs.

This FAQ is divided into the following areas:

I. Compliance and Certification

Q: Under what circumstances does my library have to comply with CIPA?

A: Your library will have to comply with CIPA when using either of the federal programs below for the purposes listed.

Program	***CIPA Compliance Needed***	***CIPA Requirements Do Not Apply****
E-rate	When getting discounts for • internal connections • Internet access	When getting discounts for • telecommunication services (voice or data)
LSTA	When using funds for • purchasing computers that access the Internet • paying for Internet access	When using funds for • any other purposes allowed by the program and state program guidelines

* Even under these circumstances a library must still check the "does not apply" statement on Form 486. See below for more information on this.

Q: What are the basic requirements of the law?

A: There are three basic requirements in the legislation that applicants must meet, or be "undertaking actions" to meet. The requirements are:

1. The library must use blocking or filtering technology on all computers with Internet access. The blocking or filtering must protect against access to certain visual depictions described below.
2. The library must adopt and implement an Internet safety policy that addresses the criteria described below.
3. The library must hold a public meeting, as described below, to discuss the Internet safety policy.

Q: How do we certify that we are meeting the above three requirements?

A: The E-rate Form 486 is being revised to allow applicants to make the proper certification statement. There will be three certification options on the Form 486 and applicants will have to select the option that describes their state of compliance. The three options will say, in essence, that:

Option 1: The library is in compliance with the three requirements;
Option 2: The library has not yet completed all requirements but is undertaking actions to do so by the start of Year 4 services; or
Option 3: CIPA requirements do not apply because the library receives discounts for telecommunications only.

The Indiana State Library recommends that if there is any doubt about your library's compliance status, that you select option 2 for Year 4. *Option 2 ensures your eligibility for Year 4 E-Rate discounts and allows for further time to spend reviewing all the issues.*

Remember: Checking option 2 carries the obligation to at least "undertake actions" by the time services start for Year 4 discounts (see question below).

As noted previously, CIPA also applies to the use of LSTA funds from the Institute of Museum and Library Services (IMLS). If a library receives E-Rate funding, the E-rate regulations take precedence. If the E-Rate is not used, requirements of the other agencies must be followed. These two agencies have not yet issued CIPA regulations. Based on information received from the IMLS, it appears that public libraries using LSTA funds will not have to declare their level of compliance (i.e., one of the three above options) until January 1, 2003.

Q: What happens if a library does not make any type of certification?

A: Your library will not be eligible for E-rate discounts on services until the proper certification(s) are submitted. If discounts are incorrectly awarded to a noncompliant library, the library, not the service provider, will be responsible for reimbursement. In a consortium application, any member that initially is not in compliance, or later falls out of compliance, will not be eligible for funding, but all other members of the consortium that are in compliance retain their eligibility.

Q: What is the certification timeframe for the E-rate's Year 4?

A: The newly modified Form 486 should be filed according to its usual schedule. This is generally within ten days of receiving the Funding Decision Commitment Letter (FDCL) or start of services, but in no case later than October 28, 2001, for Year 4 funding. Note: Some Year 4 applicants may not get a Funding Decision Commitment Letter by October 28. Also, some Year 4 services may not start until after October 28. The FCC and SLD are aware of these possible situations and they will take action at a later date to address them.

Q: I keep hearing about the need to do something by July 1, 2001. What has to be done by this date?

A: If your library (most Indiana public libraries) will be getting discounts on Internet access or internal connections, and the discounts will start on July 1, 2001, then you must certify on either Form 479 (for Internet access through Intelenet) or Form 486 that your library either meets the CIPA requirements (option 1), or that you are "undertaking actions" to meet the requirements (option 2) *by the July 1 date*. In other words, in such instances even if Form 479 or 486 is not completed until mid-September, the CIPA compliance option you check is retroactive back to the start of services.

Very few applicants will get discounts on Year 4 "internal connections." However, most Indiana's libraries will get discounts for Internet access, and in almost all instances the discounts

start July 1, 2001. *Thus these libraries must meet all CIPA requirements or be "undertaking actions" to meet the requirements by July 1, 2001.* "Undertaking actions" requires some positive, documented action. See the SLD Web site for examples of actions to take. Some of these are

- having staff meetings to discuss compliance issues
- appointing a committee to review compliance issues (filtering, AUP changes, etc.)
- discussing the issue with your board
- making inquiries for information from filtering vendors
- attending CIPA-related programs at the ALA conference

You should document the dates of any meetings or discussions, keep copies of the agendas, note any actions taken, etc. Retain all documentation for your records.

An applicant that, in good faith, certifies on Form 486 that it is "undertaking actions" but later during Year 4 decides that it cannot or will not meet the requirements of the law by July 1, 2002, will not be eligible for discounts on Internet access or internal connections in Year 5 (July 1, 2002). The library will still be able to receive such discounts during Year 4.

The ALA and ACLU filed legal challenges to the CIPA requirements in federal court in March 2001. The suit is on behalf of public libraries only. The case will not be decided until many months into the Year 4 funding cycle. Libraries wanting to receive Year 4 funding should definitely follow through on the process and make the proper certification as outlined above. (See the ALA CIPA Web site for more information on this.)

Q: Who makes the certification?

A: The E-rate's Billed Entity (e.g., a library, or Intelenet) completes Form 486. The newly added CIPA certification section of Form 486 notes that the library board, or other authority who administers the library does the certification. This "other authority" will most often be the library director, or any other staff member who has significant administrative authority.

For libraries that are part of a consortium application, the Form 486 certification is submitted to the SLD by the Billed Entity on behalf of members of the consortium (Intelenet). Each member of the consortium must complete the new E-rate Form 479 declaring its compliance with CIPA. The certification language on Form 479 will parallel the language found on Form 486. Each member of the consortium must submit a signed Form 479 to the Billed Entity. The 479 forms are not submitted to the SLD but are kept on file by the Billed Entity. (These new forms have not been released by the FCC yet.)

Q: What will be needed for Year 5 compliance?

A: After year 4, a statement of compliance will need to be made every year when Form 486 is filed. Technically, an applicant needs to comply with CIPA requirements only during the E-rate years in which discounts are received for Internet access and internal connections. It is possible, but not likely, for an applicant to go in and out of compliance in response to the type of discounts it receives.

If an applicant receives discounts on Internet costs and internal connections in Year 4 and will be getting such discounts in Year 5, it must meet the requirements for option 1 by the time Year 5 services start. In other words, option 2 ("undertaking actions") will not be a valid option for Year 5 under such circumstances. If an applicant *did not receive* discounts on Internet costs or internal

connections in Year 4, but has requested and will be getting such discounts in Year 5, then option 2 ("undertaking actions") would be a valid option to select by the time Year 5 services start.

II. The Three Basic CIPA Requirements

Below are several questions and answers related to the three basic CIPA requirements:

1. Technology Protection Measure (Filtering)
2. Internet Safety Policy
3. Public Meeting on the Internet Safety Policy

1. Technology Protection Measure (Filtering)

Q: Which computers have to be filtered?

A: The law states that *all* computer workstations that can access the Internet must have some type of blocking or filtering technology in place. (In the law this is known as a "technology protection measure.") This includes student, staff, administrative, and patron workstations accessed by minors or adults. Under certain circumstances there is a provision that allows filters to be disabled as described in the next question.

Q: Does the filter have to be active at all times for everyone?

A: The law states that an administrator, supervisor, or other authorized person may disable the filter to allow Internet access for lawful purposes. (Note: Even without CIPA, there is no constitutional protection to allow viewing of obscene pictures, and child pornography, regardless of its medium, is clearly illegal.)

The law does not give a person the right to have filtering disabled, rather it gives permission to authorized school or library staff to disable the filter for lawful purposes. Note: In the Loudoun case (Mainstream Loudoun, et. al. vs. Board of Trustees of the Loudoun County Library) filtering all workstations at all times was found to be unconstitutional on first amendment grounds. This case is referenced in the ALA's legal action against CIPA.

How the disabling is to be done, both technically and from a procedural and policy perspective, is a local school or library decision. The law provides no other guidance on how this can be done, and the FCC declined to provide any further clarification in this area, saying it was a local decision. The filter disabling provision in the TLCF and LSTA sections of CIPA apply to both adults and minors. Under the E-rate section, the disabling provision applies only to adults. There is no provision in the E-rate language that allows unfiltered access by minors for any purpose.

Q: What has to be filtered?

A: The law requires filtering of visual depictions of

1. obscenity,
2. child pornography, and
3. materials harmful to minors (minors only).

The law *does not* require the filtering of text.

Q: What are the definitions of obscenity, child pornography and harmful to minors?

A: These terms are defined in the act as follows:

1. "Obscenity" is defined in a reference to section 1460 of title 18, U.S. Code
2. "Child pornography" is defined in a reference to section 2256 of title 18, U.S. Code
3. "Harmful to minors" is defined in CIPA and means any picture, image, graphic image file, or other visual depiction that, with respect to minors:
    a. taken as a whole, appeals to a prurient interest in nudity, sex, or excretion;
    b. depicts, describes, or represents, in a patently offensive way, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
    c. taken as a whole, lacks serious literary, artistic, political, or scientific value.

The FCC declined to further define obscenity, child pornography, and the term "harmful to minors" beyond what is already stated in the law.

Q: How effective do the filters have to be? Is there any type of effectiveness certification for the filter?

A: It is important to note that the law states that filters must *protect* against visual depictions outlawed by the legislation. The filter does not have to *prevent* access to all such depictions. (No filter is 100% effective in preventing all such access.) In developing the CIPA regulations, the FCC declined to further define the filter requirements or to adopt any type of definition or certification on how effective a filter must be, beyond the very general "protect" language of the law. Thus, there is no such thing as an FCC certified "CIPA compliant filter."

Furthermore, the FCC indicated that it will not mandate that libraries track the number of attempts made to access prohibited visual depictions or the number of times the filter succeeds or fails. It also will not require libraries to collect any complaints filed by the public. (The library's Internet policy may indicate that it will track and collect such statistics but there is no mandate to do this in the law or regulations.)

To help determine how effective filters are, the law requires that by June 2002 the National Telecommunications and Information Administration (NTIA) will initiate a process to evaluate Internet blocking and filtering programs.

Q: What are the legal implications if the filter occasionally allows banned visuals to appear on the screen?

A: As noted above, the law states that filters must *protect* against visual depictions outlawed by the legislation, they do not have to *prevent* access to all such depictions. The FCC presumes that Congress did not intend to penalize libraries that act in good faith and in a reasonable manner to implement filters. The FCC also notes that failure to comply with the law's requirements, "could also engender concern among library patrons and parents of students at the school. We believe that libraries will act appropriately in order to avoid such outcomes" [FCC regulations, par. 47]. In other words, the FCC will rely, in part, on community "concern" to serve as one mechanism to enforce compliance. It is most likely that any community concern will be related to the filtering issue.

In instances where an individual or group believes the library is in violation of CIPA (e.g., too many banned images get through the filter), it is the opinion of the some attorneys that no individual or group has grounds under the law to initiate a legal action directly against the library. In such instances, any complaints about compliance would be made to the FCC, and the FCC would then decide whether to take action, such as withdrawing the applicant's discounts. The FCC is reviewing the need for it to take any action under such circumstances, although it assumes that it will "rarely, if ever," be called upon to do so.

Q: Do we have to forbid Web-based email or access to chat rooms?

A: Your handling of any Web-based email and chat rooms is a local matter to be decided by your staff, administration, or board. There are products available that will block access to all graphics attached to emails and to graphics that may be appended to chat room messages. Proper use of email, chat rooms, and other Internet services must be addressed in the Internet Safety Policy (a.k.a., Acceptable Use Policy) per the language in N-CIPA.

Q: Can we use E-rate funding to pay for filtering software or services?

A: E-rate funds cannot be used to pay for filters. LSTA funds are permitted by federal law to be used for purchasing filters, but the state's LSTA Advisory Committee and the Indiana State Library have not agreed that LSTA funds should or should not be used to purchase filters.

Q: Can filtering be done centrally by an Internet Service Provider (ISP) or at the library server level (LAN or WAN), or does the filter have to be individually installed on each workstation?

A: It makes no difference where the filtering is done – whether at the ISP, at the LAN or WAN, or at the individual workstation. The filter, regardless of where it is located on the network, must protect against the visual images outlawed in the legislation. (Whether the library decides to filter other content is a local decision.) The option to install filtering software on each individual PC works best with a very limited number of PCs. The option to filter at some point higher in the network is more efficient when filtering a large numbers of workstations, but you may have a limited ability to customize settings for each workstation. Note: With filtering at the ISP, LAN, or WAN level, it may take some network reconfiguration to allow the filter to be disabled periodically as allowed in the law.

2. Internet Safety Policy

Q: Can we use our already adopted Acceptable Use Policy (AUP) as the CIPA Internet safety policy?

A: You can use your current AUP if it meets all the requirements as stated in the legislation. If, after reviewing your AUP, you determine that it does not meet the law's requirements, then you will have to initiate a process to revise it so that it is in compliance.

Q: What must be included in our AUP to be in compliance with the law?

A: The CIPA section of the law says that a library must have an Internet safety policy in place and this policy must include the use of filters to protect against the access to the visual depictions outlawed in the act. The law does not require monitoring provision in the library's policy. Note: The law and FCC rules do not require the actual tracking of Internet use by minors or adults.

The N-CIPA section of the law is much more specific in its safety policy requirements. N-CIPA requires that libraries participating in the E-Rate program adopt and implement an Internet safety policy that addresses:

1. Access by minors to inappropriate matter on the Internet and the Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minors' access to materials harmful to minors.

The above five areas do not apply to the use of LSTA funds that are subject to the other basic CIPA requirements (i.e., need for filtering and hold a public hearing).

The Internet Safety Policy must be adopted after holding at least one public hearing or meeting. (See the Public Meeting section below.)

Q: One of the requirements refers to access by minors to "inappropriate matter" and another refers to access to "materials harmful" to minors. What's the difference?

A: The term "harmful to minors" is defined in CIPA and referenced previously in this FAQ. The definition of "inappropriate for minors" is to be made by the library board or administration. The law states specifically that the federal government is not to make any determination on what is, or is not, "inappropriate for minors."

Q: Who is considered a minor?

A: CIPA defines a minor as any person less than 17 years of age.

Q: Does the Internet Safety Policy have to be adopted by the library board or can it be done as an administrative procedure?

A: The law says the "library" shall adopt and implement a policy that meets the requirements of the law. Though the law does not state specifically that the policy must be passed by the board, the Indiana State Library strongly encourages board action on it.

3. Public meeting on the Internet Safety Policy

Q: Can a regular meeting of the library board be used as the "public meeting" required by CIPA?

A: The law and the regulations give libraries considerable flexibility in meeting the public hearing mandate. The law says simply that libraries must "provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy." The FCC's regulations do not elaborate any further on this issue. Considering the lack of more specific language in this area, the Indiana State Library believes that the public hearing can be held in conjunction with a regular board meeting. Notices of such a meeting must comport with the state's open meetings law. Any notice should clearly state that there will be a time for public comments regarding the Internet policy. Another option is to have a wholly separate meeting

where comments from the public are taken. Be certain to document fully any such public meeting by keeping a copy of the notice, any minutes of the meeting, any actions taken, etc.

III. Sources for More Information

If you need more information, contact Martha Roblee, 800-451-6028, fax 317-232-0002, marthar@statelib.lib.in.us

Readers are encouraged to review the following Web resources.

ALA CIPA Site <http://www.ala.org/cipa>

- Good site with the latest legal and regulatory information, etc.

The Wisconsin DPI Site on CIPA and Filtering
<http://www.dpi.state.wi.us/dlcl/pld/filtering.html>

- A set of PowerPoint slides on CIPA and filtering.

Children's Internet Protection Act (CIPA)
<http://www.cdt.org/legislation/106th/speech/001218cipa.pdf>

- The text of the legislation, both CIPA and N-CIPA.

FCC CIPA Regulations
<http://www.fcc.gov/Daily_Releases/Daily_Business/2001/db0405/fcc01120.doc>

- These are the FCC's regulations released April 5, 2001. The regulations outline the specific actions that schools and libraries must take to comply with CIPA and N-CIPA when using E-rate for internal connections or Internet access.

SLD Specific CIPA Guidance for Year 4 "Undertaking Actions" Certification
<http://www.sl.universalservice.org/whatsnew/MISC/CIPA051801.asp>

- A good review of the "undertaking actions" issues and a listing of the types of actions that can be taken to meet the Year 4 requirements.

6-7-01